ITEA Journal 2009; 30: 57–64
Copyright © 2009 by the International Test and Evaluation Association

Capabilities in Context: Evaluating the Net-Centric Enterprise

Steve Bridges and Danielle Mackenzie
Joint Interoperability Test Command Fort Huachuca, Arizona
Kathleen Powers and Jonathan Snyder
Northrop Grumman Mission Systems,
Fort Huachuca, Arizona

Traditional interoperability testing focuses on the operational effectiveness of preplanned information exchanges to and from the capability being tested as well as functionality of the capability to perform its mission objectives. As the Department of Defense continues to migrate to a net-centric architecture, standalone systems will be replaced with service-based capabilities deployed in various enterprises. In this context, a capability inherits both the risks and requirements associated with that enterprise. The relationship between a capability and the enterprise on which it is deployed is symbiotic and, as such, requires an evaluation of capability functionality as well as the ability of the enterprise to support the capability's mission-driven business processes.

Key words: Net-centric enterprise; enterprise-level test approach; information sharing; operational suitability; effectiveness; survivability; requirements; metrics.

The Department of Defense (DoD) test community has a long history of "program-level" interoperability testing. Current methods focus on assessing information exchanges for operational effectiveness, but do not include an assessment of the enterprise architecture components. The enterprise is a community of systems and services (e.g., people, organizations, and technology) that are interdependent and must coordinate functions and share information in support of a common mission or a set of related missions. This test philosophy cannot support a net-centric DoD where decision making is based on tiered accountability and federated governance. In the net-centric enterprise, the line between "mine" and "yours" no longer exists. Investments are still made based on capability gaps, but only after the benefits of reuse and loose coupling are fully exploited through the application of service-oriented architecture (SOA) best practices. The tester must look at the enterprise holistically and determine when it comes to net centricity, how are we doing?

Introduction

The Defense Information Enterprise Architecture (DIEA) v1.0 (April 2008) describes the DoD net-centric vision as follows[1]:

> *"To function as one unified DoD Enterprise, creating an information advantage for our people and mission partners by providing:*
>
> - *A rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise;*
> - *An available and protected network infrastructure (the Global Information Grid (GIG)) that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities."*

As testers, how do we ensure that the DoD does, in fact, operate as one seamless and interoperable enterprise, even while implementing a tiered accountability decision model and a federated governance structure?

JITC proposes a test approach *(Figure 1)* that includes all of the components of an enterprise that are required to ensure success. However, not all requirements in the test approach will apply to every enterprise. The test approach should therefore be tailored to meet the needs of each unique enterprise. This approach aligns with DIEA objectives, imple-

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Capabilities in Context: Evaluating the Net-Centric Enterprise	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Interoperability Test Command,P.O. Box 12798,Fort Huachuca,AZ,85670-2798**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**8**	

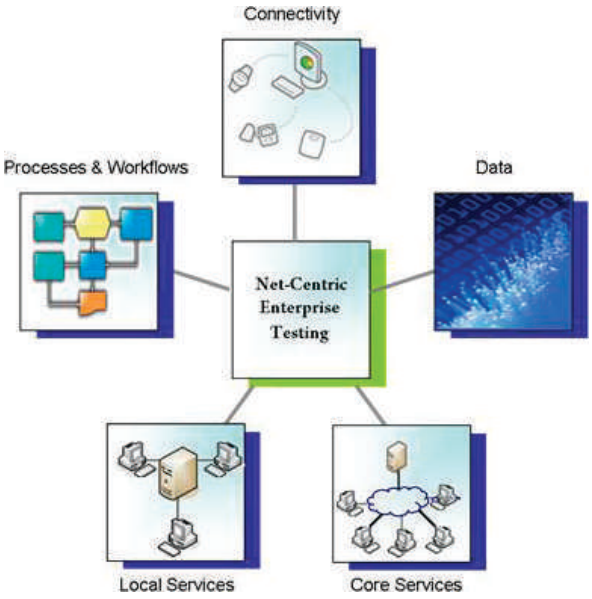

Figure 1. Net-centric enterprise testing approach.

ments best-of-breed practices from industry and academia, and provides value-added information to DoD capability portfolio managers, enterprise architects, and program managers for decision making. This approach provides technical rigor, flexibility, and scalability required to ensure testing provides value-added information within the cost and schedule constraints of rapid acquisition initiatives.

Connectivity

Connectivity refers to the hardware and software implementations that enable connection between clients and servers, between services, and among networks *(Figure 1)*. These implementations comprise the enterprise network infrastructure and support the mission-critical and mission-enabling (nonmission-critical) information exchanges between capabilities on the enterprise to include clients, servers, services, and networks.

Requirements

Compliance with the DIEA requires that the connectivity of the enterprise support capability missions by providing secure, dynamic, computing-platform agnostic and location-independent data storage, real-time provisioning, allocation of shared resources, and access to shared spaces and information assets within the mission-required Quality of Service (QoS) parameters.

Metrics

The following measurements comprise the suggested minimum set of metrics needed to support an enterprise connectivity assessment. However, this list should be tailored to accommodate each unique enterprise by either deleting nonapplicable metrics or adding new metrics.

Operational availability (A_o). Testers will review logs captured with an enterprise service management tool and verify the operational availability of the network connections. This is determined by using the operational availability equation [A_o = Mean Time between Failure (MTBF)/MTBF + Mean Time to Repair (MTTR)] and is represented as a percentage.[2]

Lowest throughput (in GB/s). This metric indicates availability of the network by measuring the lowest throughput speed at all nodes during normal message request load on the enterprise. A network experiencing lowered throughput may result in slow message exchanges that delay service access or interruptions in service access, which prevent function. Using a network loading tool, testers will simulate network load with a normal random distribution over time and measure the throughput speeds at all nodes. If the lowest throughput speed does not meet mission-critical threshold requirements, then the enterprise cannot support the mission.

Bandwidth usage. This metric indicates overall network load capacity. Bandwidth usage data are collected by enterprise service management tools and enterprise logs. The data traffic is then compared with the total data resources available. Testers will verify that the bandwidth used by the capabilities on the enterprise do not exceed the set limits defined in the foundational documentation. Measurements should focus on high traffic services and large data output services using realistic network load distributions over time.

Core Services

Core services are ubiquitous, common solution services that provide capabilities essential to the operation of the enterprise.[3] They are infrastructure-type capabilities that support multiple key consumers. Examples of core services include:

- security and authentication services,
- orchestration services,
- load monitoring services,
- load balancing services,
- messaging services,
- service configuration monitoring tools,
- enterprise service management tools,
- enterprise test tools,
- enterprise service bus capabilities.

Core service testing will target the core services that are available on the enterprise and will focus on their net-centric performance and design in support of capability mission requirements.

Requirements

Compliance with the DIEA requires that the core services deployed on a given enterprise support the mission by implementing a loosely coupled architecture that is visible, accessible, understandable, and trusted by both anticipated and unanticipated users. Core services must support mission requirements even during Disconnected, Intermittent, or Limited (DIL) bandwidth conditions and ought to provide Network Operations (NetOps) related data, such as performance and availability, to ensure compliance with GIG service level agreements (SLAs).

Metrics

The following measurements comprise the suggested minimum set of metrics needed to support an enterprise core services assessment. However, this list should be tailored to accommodate each unique enterprise by either deleting nonapplicable metrics or adding new ones.

Operational availability (A_o). Testers will review logs captured with an enterprise service management tool and verify the operational availability of enterprise core services. This is determined by using the operational availability equation (A_o = MTBF/MTBF + MTTR) and is represented as a percentage.[4]

Maximum latency (response time) for average request (in ms). Time difference between requestor's service request and service response (measured from time of service request [received at service provider] to time of response [sent from service provider]). Testers will test core service maximum latency to determine whether mission-critical threshold requirements for response times have been met.

Idempotency (in a stateless client). This metric indicates the uniformity of the responses from the core service. If the service client is stateless, then the response received after executing a service call should be the same no matter how many times the service call is executed.[5] Testers should send a statistically significant number of identical service calls (messages) to the core service and verify that identical responses are received.

Data accuracy. Core services that provide data should provide a quantifiable measurement of data accuracy. A capability could have varying degrees of accuracy requirements. Enterprise core services must, as a threshold requirement, support the highest level of mission-critical accuracy required by enterprise capabilities that will utilize those core services.

Maximum size of user domain. This metric indicates scalability of service, i.e., how well the core services can support the user domains required by the sum total of all missions executed in the enterprise.

Maximum number of simultaneous users. This metric identifies the maximum number of concurrent users performing "normal" operations beyond which A_o or throughput falls below acceptable levels. It indicates scalability of core service and consistency of performance under varying load conditions. The threshold requirement for each enterprise core service must represent the sum of the average number of concurrent users required by all supported capabilities deployed on the enterprise.

Local services

Local services are application-type capabilities that provide a function in support of an operational requirement or mission. Local services may vary from extremely small bits of capability (provides a map) to large capabilities drawn from service enabling a stovepiped legacy system.

Local service testing focuses on both the functionality of capabilities on the enterprise, as well as compliance with inherited enterprise requirements.

Requirements

Compliance with the DIEA requires that the local services deployed on a given enterprise support the mission by implementing a loosely coupled architecture that is visible, accessible, understandable, and trusted by both anticipated and unanticipated users. Local services must provide access to authoritative data assets, services, and applications, and be accessible to all authorized users except where limited by law, policy, security, classification, or operational necessity. Local services must support graceful degradation of capability and performance during DIL conditions and ought to provide NetOps related data, such as performance and availability, to ensure compliance with GIG SLAs.

Metrics

The following measurements comprise the suggested minimum set of metrics needed to support an enterprise local services assessment. However, this list should be tailored to accommodate each unique enterprise by either deleting nonapplicable metrics or adding new metrics.

Service visibility. Testers will ensure that local service is registered in the enterprise service registry and is "discoverable" with an intuitive keyword search using the enterprise's federated search capability.

Service accessibility. Testers will ensure that local service has written policy listing actions necessary to gain transparent machine-to-machine access to services via user level credentials, system level credentials, or trust relationships (e.g., SLAs). This includes users who are anticipated (i.e., known users with specific missions that have been granted access to the system), unanticipated (i.e., users without specifically defined missions who have been granted access to the system), and unauthorized users (i.e., users without access to the system). Policy must be registered in the service's submission package located in the DoD Metadata Registry, and policy must be enforced as written.

Service understandability. Testers will ensure that the local service Web Services Description Language correctly executes service operations and any community of interest (COI) or Enterprise mandated vocabularies and schemas are used and implemented correctly.

Service reuse. Existing enterprise services and end-user interfaces shall be used whenever possible, practical, and appropriate instead of recreating those assets.[6]

Functional requirements. Local services used by the warfighter or capability must provide functional capabilities as described in the U.S. Joint Forces Command–maintained Joint Common System Functions List (JCSFL). The JCSFL provides a common lexicon for system Command and Control (C2) functionality, including the traceability of Military Service C2 functions to their joint equivalent, for interoperability and comparative analyses. The JCSFL describes the C2 functionality of any platform, program of record, system, subsystem, component, or application that provides such functionality. The JCSFL also contains intelligence, surveillance, and reconnaisance functions and will be updated to include net-centric communications functionality, as determined by the net-centric Capability Portfolio Manager. Support functions, including those for maintenance, logistics, medical, personnel, training, etc., will be included in future revisions.[7]

Operational availability (A_o). Testers will review logs captured with an enterprise service management tool and verify the operational availability of local services to each client capability. This is determined by using the operational availability equation (A_o = MTBF/MTBF+MTTR) and is represented as a percentage.[8]

Maximum latency (response time) for average request (in ms). This metric is the time difference between requestor's service request and service response (measured from time of service request [received at service provider] to time of response [sent from service provider]). Testers will test local service maximum latency to determine whether mission-critical threshold requirements for response times have been met.

Data accuracy. Local services that provide data should provide a quantifiable measurement of data accuracy. Local services must, as a threshold requirement, support the highest level of mission-critical accuracy required by the client capability.

Maximum size of user domain. This metric indicates scalability of service, i.e., how well the local service can support the user domains required by the sum total of all missions executed in the enterprise.

Maximum number of simultaneous users. Identifies the maximum number of concurrent users performing "normal" operations beyond which A_o or throughput falls below acceptable levels. This metric indicates scalability of local service and consistency of performance under varying load conditions. The threshold requirement for the local service must represent the sum of the average number of concurrent users required by all supported capabilities deployed on the enterprise.

Graceful capability degradation. This metric identifies local service ability to implement graceful degradation capabilities as outlined by mission requirements. Mission requirements ought to specify capabilities required under varying levels of DIL bandwidth conditions. Testers should evaluate local services under conditions specified to ensure that threshold capability requirements are met.

Data

Data testing will target the data assets that are shared within the enterprise and will focus on the ability of those assets to support mission-critical threshold capability requirements. There are two types of data: content data and metadata.

Content data are data provided by a capability that provides information usable by other capabilities or users. Content data address the needs of the COIs and users or warfighters directly. A capability generally generates, transforms, stores, or consumes content data.

Metadata are data that describe the characteristics of the capability or data exposed on the enterprise. Metadata generally describe content data and/or services that are available for consumption, e.g., what standards the service or data asset follows, how to use the service or data asset (for machine-to-machine interface), and how to discover the service or data.

Requirements

Compliance with the DIEA requires that the data deployed on a given enterprise support the mission by being visible, accessible, understandable, and trusted by both anticipated and unanticipated users. Data should follow the syntax and semantics as defined by the associated community of interest and should be appropriately tagged using the enterprise standard for discovery metadata (DoD Discovery Metadata Specification).

Metrics

The following measurements comprise the suggested minimum set of metrics needed to support an enterprise data assessment. However, this list should be tailored to accommodate each unique enterprise by either deleting nonapplicable metrics or adding new metrics.

Data visibility. Testers will ensure that discovery metadata are registered in an Enterprise Catalog in accordance with DDMS, thus making it discoverable within the targeted enclave. Testers will ensure that data are "discoverable" with an intuitive keyword search using the enterprise's federated search capability.

Data accessibility. Testers will ensure that Federated Search results provide active link (e.g., Uniform Resource Locator) that points to the specified data asset within the targeted security enclave. Testers will ensure that the data provider has written policy listing actions necessary to gain transparent user access to the data via user level credentials, system level credentials, or trust relationships (e.g., Access Control List). This includes users who are anticipated (i.e., known users with specific missions that have been granted access to the system), unanticipated (i.e., users without specifically defined missions who have been granted access to the system), and unauthorized users (i.e., users without access to the system). Policy information must be registered in an *enterprise catalog*, include the steps by which a user may request access to the data, and be available within "2 clicks" from the active link provided by Federated Search.

Data understandability. Testers will ensure that data are navigable within the limitations of the interface, are labeled with meaningful labels, are conveyed effectively, and use commonly understood language that conforms to COI-approved vocabularies.

Semantic reuse. Semantic vocabularies shall reuse elements of the DoD Intelligence Community (IC)-Universal Core information exchange schema.[9]

Data reuse. Existing enterprise data shall be used whenever possible, practical, and appropriate, instead of recreating those assets.[10]

Data accuracy. Data should provide a quantifiable measurement of accuracy. Data that are provided as a service should maintain source level of accuracy in accordance with mission-critical threshold requirements.

Data refresh rate. Data must maintain a refresh rate that is compliant with the threshold mission requirements for the client capability.

Graceful degradation. Data must be accessible during DIL bandwidth conditions. Data redundancy should be made available through the use of local caching and data storage. Data should be appropriately tagged with "age" or "time of last refresh" information so that the user or warfighter is aware of the currency of the data for decision making purposes.

Processes and workflows

A *process* is a composition of one or more types of services that are capable of accomplishing a particular part of a mission objective *(Figure 1)*. For example, "perform capability A, translate the results, then perform capability B" is a *process*. A *workflow* is a specific composition of processes and services that will accomplish a mission objective. For example, "service A calls translation service AB, which calls service B" is a *workflow*.

Processes and workflows testing will target the business processes that combine to form workflows to accomplish capability mission objectives.

Requirements

Process and workflow requirements should be derived from joint mission threads developed by the user representative for a given capability. Mission threads should provide operational activities, tasks, and required performance characteristics needed to meet threshold mission-critical requirements. Mission threads will be decomposed into the materiel and nonmateriel solutions required to execute the thread. The processes and workflows required to execute a given mission are best represented using dynamic modeling techniques such as business process modeling notation.

Metrics

The following measurements comprise the suggested minimum set of metrics needed to support an enterprise processes and workflows assessment. However, this list should be tailored to accommodate each unique enterprise by either deleting nonapplicable metrics or adding new metrics.

Operational effectiveness. Operational effectiveness is the overall degree of mission accomplishment of a system when used by representative personnel in the environment planned or expected for operational employment of the system considering organization, doctrine, tactics, survivability, vulnerability, and threat. The evaluation of operational effectiveness is linked to mission accomplishment. The early planning for the evaluation should consider any special test requirements, such as the need for large test areas or ranges or supporting forces, requirements for threat systems or simulators, new instrumentation, or other unique support requirements.

Operational suitability. Operational suitability is the degree to which a system can be satisfactorily placed in field use, with consideration given to reliability, availability, compatibility, transportability, interoperability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistics supportability, documentation, training requirements, and natural environmental effects and impacts. Early planning for the suitability evaluation should include any special needs for number of operating hours, environmental testing, maintenance demonstrations, testing profiles, usability of developmental testing data, or other unique test requirements. Operational suitability should be evaluated in a mission context to provide meaningful results. For example, maintaining a required Operations Tempo over an extended period while conducting realistic missions gives insight into the interactions of various suitability factors, such as the ability to maintain stealth features during sustained operations.

Operational survivability. Operational survivability is the degree to which a capability is able to resist or recover from detrimental effects. Measurement time frames should be from the start of unavailability to the time when service is restored. The enterprise should have automated tools in place to restore service automatically after service is lost.

Summary

This enterprise-level test approach provides the basis for evaluating a net-centric enterprise by examining the individual capabilities in context with the components of their parent enterprise: connectivity, core services, local services, data, and processes and workflows.

"Program-level" interoperability testing does not reveal problems that will occur as a result of the growing intricacy of client–service dependencies, changing interface requirements, and resource scaling issues as the enterprise (and its resident service, data and infrastructure assets) matures and multiplies. "Program-level" interoperability testing also does not reveal the benefits of reuse and loose coupling that may be achieved by the enterprise through the application of SOA best practices.

In contrast, this enterprise-level test approach will expose interservice dependencies and shortcomings and highlight the benefits of existing enterprise infrastructure and SOA governance assets that promote efficiency, enable development, and manage growth of net-centric technologies. ❑

Steve Bridges is the chief engineer for the Joint Interoperability Test Command (JITC). In this capacity, he is responsible for the oversight of technical aspects of all JITC test programs, development of new test methods for the net-centric environment, and modernization of both test infrastructure and instrumentation. He serves as adviser to the JITC commander on all technical issues. He has worked on government technical acquisition projects for over 35 years. He received his bachelor of science degree in electrical engineering from Texas A&M, Kingsville, in 1972 and was a recipient of the Defense Information Systems Agency (DISA) Director's Award for Achievement in Scientific/Engineering Field. E-mail: steve.bridges@disa.mil

Danielle Mackenzie works in JITC's Strategic Planning and Engineering Division as the Net-Enabled Command Capability (NECC) Capability Test Team lead. She has 10 years of experience in both government and industry, focusing on the research, development, engineering, test, and evaluation of command and control systems. Ms. Mackenzie holds a bachelor's degree in mathematics from the College of Saint Elizabeth, Morristown, New Jersey, and a master's degree in systems engineering from Stevens Institute of Technology, Hoboken, New Jersey. Previous assignments at Fort Monmouth's Communications-Electronics Research, Development and Engineering Center (CERDEC) include Project Lead for the Network Enabled Battle Command (NEBC) program, and Information Management Integrated Product Team lead for the Objective Force Warrior program. A member of the Defense Acquisition Corps, Ms. Mackenzie holds Level III DAWIA certification in Systems Planning, Research, Development and Engineering Mackenzie@disa.mil

Kathleen Powers works for Northrop Grumman Mission Systems as a senior systems engineer supporting

JITC's Strategic Planning and Engineering Division. She has fifteen years of experience in communications and systems engineering, focusing on signal processing software development as well as test and evaluation processes. Ms. Powers holds a bachelors degree in electrical engineering from Clarkson University, Potsdam, New York, and a masters degree in electrical engineering from Johns Hopkins University, Baltimore, Maryland. Ms. Powers is a member of the Institute of Electrical and Electronics Engineers and holds a U.S. patent for a "System for recognizing signal of interest within noise." E-mail: Kathleen.Powers.ctr@disa.mil

JONATHAN SNYDER works for Northrop Grumman Mission Systems as a test engineer supporting JITC's Strategic Planning and Engineering Division. He has fourteen years of experience in both government and industry focusing on operations, test and evaluation, and deployment of hardware and software networks. Mr. Snyder holds a bachelors degree in information technology and a masters degree in computer information systems from the University of Phoenix, Tucson, Arizona. Mr. Snyder served five years in the U.S. Army as an automated communications computer repair technician and seven years as a technician for a long distance telecommunications provider. E-mail: Jonathan.Snyder.ctr@disa.mil

Endnotes

[1]DoD Office of the Chief Information Officer, Defense Information Enterprise Architecture, Version 1.0, April 11, 2008, http://www.defenselink.mil/cio-nii/docs/DIEAv1.pdf.

[2]http://src.alionscience.com/pdf/RAC-1ST/OPAH(1st).pdf.

[3]http://nesipublic.spawar.navy.mil/nesix/View/GL1138.

[4]http://src.alionscience.com/pdf/RAC-1ST/OPAH(1st).pdf.

[5]http://doi.ieeecomputersociety.org/10.1109/ISPAN.1999.778951.

[6]DoD Office of the Chief Information Officer, Defense Information Enterprise Architecture, Version 1.0, April 11, 2008, http://www.defenselink.mil/cio-nii/docs/DIEAv1.pdf, p. 11.

[7]Chairman of the Joint Chiefs of Staff Instruction 6212.01E DRAFT—Staffing Copy, https://www.intelink.gov/wiki/Portal:CJCSI_6212_Revision.

[8]http://src.alionscience.com/pdf/RAC-1ST/OPAH(1st).pdf.

[9]DoD Office of the Chief Information Officer, Defense Information Enterprise Architecture, Version 1.0, April 11, 2008, http://www.defenselink.mil/cio-nii/docs/DIEAv1.pdf, p. 11.

[10]DoD Office of the Chief Information Officer, Defense Information Enterprise Architecture, Version 1.0, April 11, 2008, http://www.defenselink.mil/cio-nii/docs/DIEAv1.pdf, p. 11.

Bibliography

Ananiev, Alexander. June 17, 2007. Comparison of SOA suites. *MyArch*. http://myarch.com/comparison-of-soa-suites (accessed July 14, 2008).

Anon. July 25, 1996. *The New Hacker's Dictionary*. version 4.0.0. http://www.ccil.org/jargon/ (accessed September 1, 2008).

Association for Enterprise Integration. October 12, 2006. *DoD Performance metrics to support industry confidence in shared services: A report of the Data Sharing and Services Strategy Working Group*. http://www.afei.org/documents/DS3PerformanceMetricsforShareServicesFinal101206.pdf (accessed July 25, 2008).

BEA Systems, Inc. March 2008. *Product data sheet BEA AquaLogic Service Bus 3.0*. http://www.bea.com/content/news_events/white_papers/BEA_AquaLogic_Service_Bus_ds.pdf (accessed July 14, 2008).

Boukerche, A. and S. K. Das. 1999. Scalability of a load balancing algorithm, and its implementation on an Intel Paragon. In *Fourth International Symposium on Parallel Architectures, Algorithms, and Networks, 1999 (I-SPAN '99) Proceedings*. pp. 274–279, http://doi.ieeecomputersociety.org/10.1109/ISPAN.1999.778951 (accessed August 14, 2008).

Braden, R. October 1989. Requirements for Internet hosts—communication layers. In *Connected: An Internet encyclopedia*. Edited by Brent Baccala. http://www.freesoft.org/CIE/RFC/1122/index.htm (accessed July 15, 2008).

DoDD 8320.02. 2 December 2004. *Data sharing in a net-centric Department of Defense*. http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf (accessed October 1, 2007).

Department of Defense. April 12, 2001. *Department of Defense dictionary of military and associated terms*. http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf (accessed October 1, 2007).

Department of Defense Chief Information Officer (DoD CIO). May 9, 2003. *Department of Defense net-centric data strategy*. http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf (accessed October 1, 2007).

DoD CIO. April 11, 2008. *Department of Defense Defense Information Enterprise architecture, version 1.0*. http://www.defenselink.mil/cio-nii/cio/diea/products/DIEA 1.0 - Final.pdf (accessed August 18, 2008).

DoD CIO. March 2007. *Department of Defense net-centric services strategy*. http://www.jcs.mil/j6/DoD_NetCentricServicesStrategy.pdf (accessed October 1, 2007).

DoD CIO. September 2006. *Department of Defense PDM III Core Enterprise Services findings and recommendations report*. http://www.defenselink.mil/cio-nii/docs/PDMIIICES_report_20061005U.PDF (accessed August 15, 2008).

Emerson, John July 31, 2008. JITC/Amberpoint Planning Session. Joint Interoperability Test Command.

Gouchie, Paul May 14, 2003. International Test and Evaluation Association Briefing.

Hewlett-Packard Development Company, L.P. 2007. *SOA governance best practices*.

Hewlett-Packard Development Company, L.P. May 2007. *SOA governance: Balancing flexibility and control within an SOA*.

Josuttis, Nicolai M. *SOA in practice: The art of distributed system design*.

MacVittie, Lori October 26, 2006. *Rollout: iTKO LISA 3.5, more than a pretty face*. http://www.ddj.com/development-tools/193401007 (accessed April 29, 2008).

NESI—Net-Centric Enterprise Solutions for Interoperability Public Website. June 17, 2008. Air Force Electronic Systems Center, Navy Program Executive Officer, Command, Control, Communications, Computers & Intelligence, and Defense Information Systems Agency http://nesipublic.spawar.navy.mil/ (accessed July 16, 2008).

Net-Centric Enterprise Services (NCES) SOA Foundation. *On-boarding process work-flows*. https://portal.soaf.ces.mil/soafdashboard/ (accessed September 17, 2008).

Ribarov, Lachezar, Ilina, Manova and Sylvia, Ilieva 2007. Testing in a service-oriented world. In *Proceedings of the International Conference on Information Technologies, 2007 (InfoTech-2007)*. http://www.crosschecknet.com/soa_testing/TestingInAServiceOrientedWorld.pdf (accessed July 15, 2008).

SAP Community Network. *Standards and enterprise SOA*. https://www.sdn.sap.com/irj/sdn/standards (accessed July 15, 2008).

Tilkov, Stefan July 18, 2007. *Roles in SOA governance*. http://www.infoq.com/articles/tilkov-soa-roles (accessed April 29, 2008).

Whitt, Lee July 30, 2008. Northrop Grumman Corporation (NGC) unpublished white paper written in response to Consolidated Afloat Network and Enterprise Services (CANES) SOA Request for Information (RFI). This reference was unpublished. It was written in response to the CANES SOA RFI titled, "Service Oriented Architecture in Support of the Consolidated Afloat Network and Enterprise Services (CANES) Program."